# TTP Detail – T1056.002

## TTP Information

Name: GUI Input Capture

Description: Adversaries may mimic common operating system GUI components to prompt users for credentials with a seemingly legitimate prompt. When programs are executed that need additional privileges than are present in the current user context, it is common for the operating system to prompt the user for proper credentials to authorize the elevated privileges for the task (ex: [Bypass User Account Control](https://attack.mitre.org/techniques/T1548/002)).

Adversaries may mimic this functionality to prompt users for credentials with a seemingly legitimate prompt for a number of reasons that mimic normal usage, such as a fake installer requiring additional access or a fake malware removal suite.(Citation: OSX Malware Exploits MacKeeper) This type of prompt can be used to collect credentials via various languages such as [AppleScript](https://attack.mitre.org/techniques/T1059/002)(Citation: LogRhythm Do You Trust Oct 2014)(Citation: OSX Keydnap malware)(Citation: Spoofing credential dialogs) and [PowerShell](https://attack.mitre.org/techniques/T1059/001).(Citation: LogRhythm Do You Trust Oct 2014)(Citation: Enigma Phishing for Credentials Jan 2015)(Citation: Spoofing credential dialogs) On Linux systems adversaries may launch dialog boxes prompting users for credentials from malicious shell scripts or the command line (i.e. [Unix Shell](https://attack.mitre.org/techniques/T1059/004)).(Citation: Spoofing credential dialogs)

Adversaries may also mimic common software authentication requests, such as those from browsers or email clients. This may also be paired with user activity monitoring (i.e., [Browser Information Discovery](https://attack.mitre.org/techniques/T1217) and/or [Application Window Discovery](https://attack.mitre.org/techniques/T1010)) to spoof prompts when users are naturally accessing sensitive sites/data.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: collection

**•** mitre-attack: credential-access

## Malware

* Bundlore
* Calisto
* Cuckoo Stealer
* Dok
* Keydnap
* Metamorfo
* Mispadu
* Proton
* XCSSET
* iKitten

## Tools

* SILENTTRINITY

## APTs (Intrusion Sets)

* FIN4
* RedCurl